

PARTIAL TRANSLATION OF JP 7(1995)-064911 A

Publication Date: March 10, 1995

Title of the Invention: INDIVIDUAL AUTHENTICATION SYSTEM

Patent Application Number: 5-216056

Filing Date: August 31, 1993

Inventors: Yoshiharu ENOMOTO

Applicant: SHARP CORP

(Page 2, right column, lines 46-49)

[0012] An object of the present invention is to provide an individual authentication system capable of carrying out a required check by improving the reliability of a check at each part of the system according to need.

(Page 3, left column, lines 1-9)

The invention according to claim 1 comprises: individual data registration means for registering any number of items of individual authentication data among individual authentication data for identifying an individual, such as a password, a handwriting, a fingerprint, and the like; input device selection means for selectively connecting any number of input devices among input devices for inputting respective items of individual authentication data; matching means for matching individual authentication data input by the input device with the individual authentication data registered in the individual data registration means.

(Page 3, left column, lines 19-22)

According to the invention of claim 1, a system can be configured in which only a required item is selected among plural items for identifying an individual, such as a password, a handwriting, a fingerprint, and the like.



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07064911 A**(43) Date of publication of application: **10.03.95**

(51) Int. Cl.

G06F 15/00
G06F 19/00
(21) Application number: **05216056**(71) Applicant: **SHARP CORP**(22) Date of filing: **31.08.93**(72) Inventor: **ENOMOTO YOSHIHARU**(54) **INDIVIDUAL AUTHENTICATION SYSTEM**

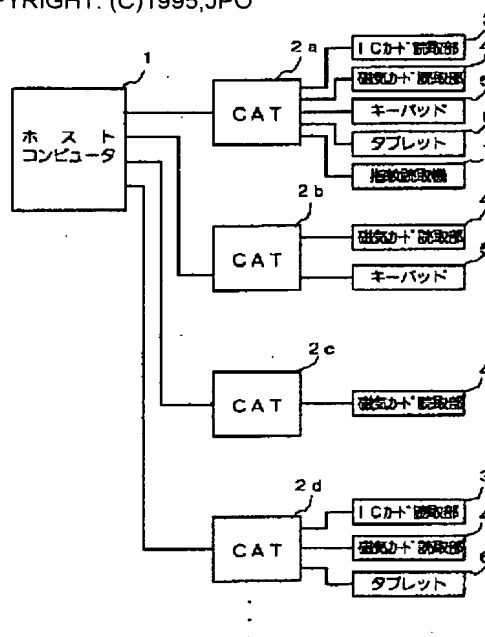
a cost.

(57) Abstract:

COPYRIGHT: (C)1995,JPO

PURPOSE: To perform high-grade authentication and to improve security by connecting only the input devices of required items and authenticating individuals by the appropriately registered individual authentication data and the appropriately selected and connected input devices.

CONSTITUTION: In respective CAT terminals 2a, 2b..., an IC card read part 3 for inserting an IC card and reading the individual authentication data as the input device and a magnetic card read part 4 for reading the data of a magnetic card are provided at need and also a key pad 5 provided with keys for inputting a password, a tablet 6 for inputting a signature and a fingerprint reader 7 for inputting a fingerprint are connected at need. The individual authentication data for authenticating the individual and individual data such as an identification number or the like are stored respectively in the IC card and the magnetic card. The individual possesses either the IC card or the magnetic card at need and uses them appropriately in the view of



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-64911

(43) 公開日 平成7年(1995)3月10日

(51) Int.Cl.⁵G 0 6 F 15/00
19/00

識別記号

3 3 0 A 7459-5L

庁内整理番号

F I

技術表示箇所

G 0 6 F 15/ 30

3 3 0

審査請求 未請求 請求項の数 3 O L (全 12 頁)

(21) 出願番号 特願平5-216056

(22) 出願日 平成5年(1993)8月31日

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 榎本 好晴

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

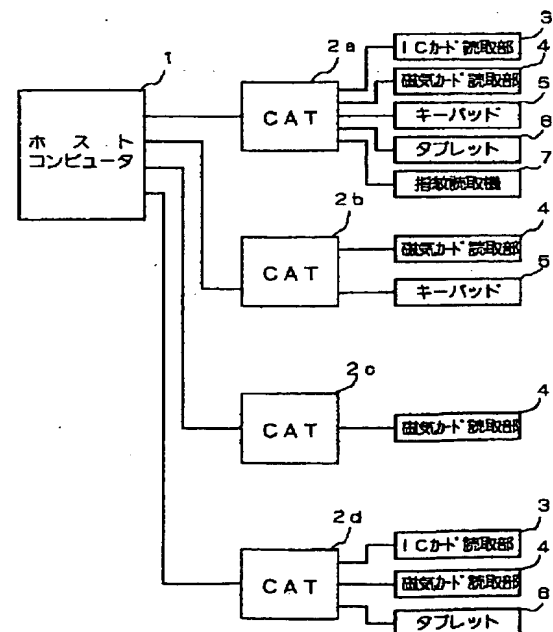
(74) 代理人 弁理士 小森 久夫

(54) 【発明の名称】 個人認証システム

(57) 【要約】

【目的】 システムの各部で必要に応じてチェックの信頼度を向上させるようにして、必要十分なチェックを行うことができるようにする。

【構成】 CAT端末2a, 2b・・・のそれぞれに必要なに応じてパスワード照合用のキーパッド5、サイン照合用のタブレット6、指紋照合用の指紋読取装置7を接続して、CAT端末の設置場所に応じて必要十分な個人認証機能を備えるとともに、多くの機能を備えたCAT端末(例えば2a)でもその場面場面で必要な機能だけを用いて個人認証を行う。



【特許請求の範囲】

【請求項 1】パスワード、筆跡、指紋等の個人を識別するための個人認証データの中から任意項目数の個人認証データを登録する個人データ登録手段と、各項目ごとの個人認証データを入力する入力装置の中から任意数の入力装置を選択的に接続する入力装置選択手段と、前記入力装置から入力された個人認証データと前記個人データ登録手段に登録された個人認証データとを照合する照合手段と、を備えたことを特徴とする個人認証システム。

【請求項 2】請求項 1 に記載の個人認証システムにおいて、前記照合手段により照合を行う項目を選択設定する照合項目選択手段を備えたことを特徴とする個人認証システム。

【請求項 3】請求項 2 に記載の個人認証システムにおいて、選択された照合を行う項目が使用不可状態であるとき、他の項目を代用する手段を備えたことを特徴とする個人認証システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、個人の正当性確認および本人確認を実施する個人認証システムに関し、例えば、クレジット処理、キャッシング処理等の金融取引時の個人認証や、企業内等での入退室チェック時の個人認証に用いられる。

【0002】

【従来の技術】従来の金融取引装置や入退室チェック装置における個人認証には次のような方法および装置が用いられていた。

【0003】① 例えば、クレジットカードにおける個人認証の場合、クレジットカードの利用者のサインを店員等のサービス提供者が目視で確認する方法で、カード上のエンボス文字をインプリントした取引証書にカード利用者がサインして、その筆跡を店員等のサービス提供者が目視で確認する方法。

【0004】② 同じくクレジットカードにおける個人認証の場合で、CAT 端末を利用し、パスワード入力用ピンパッド（通常、暗証番号の入力用としてテンキーパッドを用いる）からパスワードを入力し、それを照合する。パスワード（暗証番号）を入力し照合する方法は、銀行でのキャッシュカードによる個人認証にも用いられている。このパスワードの照合は、パスワードをカードの磁気ストライプに記しておいて端末自身がそのパスワードを読み取り照合を行う場合と、パスワードをホストが記憶しておいて回線を介して送受信を行いホスト側で照合を行う場合とがある。

【0005】③ また企業内等での入退室許可のための個人認証においても、カード上に磁気ストライプで記載されたデータを読み取る装置、キーボードから入力され

るパスワードを照合する装置、指紋入力部から入力される指紋等を照合する装置等が用いられ個人認証を行う。

【0006】

【発明が解決しようとする課題】ところが上記した従来の構成では次のような問題があった。

【0007】① 店員等のサービス提供者自身が目視でサインの照合を行う方法の場合、サインの照合には熟練が必要であり、実際のサービス提供者の数はサインの照合に熟練した者の数に到底及ぶものではないことから、盗難カード等でサインが偽造された場合のチェックはほぼ素通りの状態にある。

【0008】② ピンパッドからパスワードを入力して照合する方法では、パスワードの盗難が発生することがある。すなわち、近年では磁気的に記したパスワードを読み取ることが可能になっておりカードの磁気ストライプにパスワードを記した場合にはその盗難が比較的容易である。またパスワードとしては一般に暗証番号が用いられることが多いが、カード利用者が暗証番号を設定する場合には、生年月日等のカード利用者にとって記憶し易い番号を設定することが多く、それらのデータの盗難も比較的容易であることから、暗証番号の盗難が発生することがある。

【0009】上記したように、従来金融取引に用いられていた個人認証のシステムは比較的簡易な構成であるために不正が発生し易い。金融取引額が大きい場合にこのような不正が発生すると損害は多大なものとなる。

【0010】これを防止するために、例えば、特開昭 59-43473 号公報、特開平 3-265086 号公報に示されるように、暗証番号の照合の他に指紋照合、音声照合等の複数のチェック項目を組み合わせてチェックシステムを構築することも考えられるが、その場合には各端末に、暗証番号の入力部、指紋の入力部、音声の入力部等複数の入力部や照合部等を設ける必要があり、システムが高価になってしまう。金融取引額が大きい場合には高価なシステムを用いる価値はあるが、小額の取り引きしか行わない場合でも高価なシステムを備えるのは無駄であり、また、小額の取り引きの場合に過大なチェックを行うことは顧客に対して不快なイメージを与えるばかりでなく、時間のロスが多くなってしまふ。

【0011】一方、③に示した企業内等で入退室チェック等に用いられる個人認証システムでは、磁気ストライプを読み取る装置、パスワードを照合する装置、指紋を照合する装置等、いずれの装置を用いた場合でも、単独のチェックシステムである限りセキュリティ性の信頼度を向上させるには限界があった。

【0012】この発明の目的は、システムの各部で必要に応じてチェックの信頼度を向上させるようにして、必要十分なチェックを行うことができる個人認証システムを提供することにある。

【0013】

【課題を解決するための手段】請求項 1 に記載した発明は、パスワード、筆跡、指紋等の個人を識別するための個人認証データの中から任意項目数の個人認証データを登録する個人データ登録手段と、各項目ごとの個人認証データを入力する入力装置の中から任意数の入力装置を選択的に接続する入力装置選択手段と、前記入力装置から入力された個人認証データと前記個人データ登録手段に登録された個人認証データとを照合する照合手段と、を備えたことを特徴とする。

【0014】請求項 2 に記載した発明は、請求項 1 に記載のシステムにおいて、前記照合手段により照合を行う項目を選択設定する照合項目選択手段を備えたことを特徴とする。

【0015】請求項 3 に記載した発明は、請求項 2 に記載の個人認証システムにおいて、選択された照合を行う項目が使用不可状態であるとき、他の項目を代用する手段を備えたことを特徴とする。

【0016】

【作用】請求項 1 に記載した発明においては、パスワード、筆跡、指紋等の個人を識別するための複数の項目のうちから必要な項目のみを選択してシステムを構築することができる。すなわち、入力装置選択手段により、必要な項目の入力装置のみを接続すれば不必要な入力装置を接続する無駄がなくなり、また、個人データ登録手段により必要な項目の個人認証データのみを登録すれば不必要な登録の無駄がなくなる。そして適宜登録された個人認証データと、適宜選択接続された入力装置によって個人認証が行われる。

【0017】請求項 2 に記載した発明においては、多数の個人認証データが登録されていたり、多数の入力装置が接続されている場合であっても、その中から任意の項目が選択されてデータの照合が行われる。したがって例えば、パスワード、筆跡、指紋の 3 項目の個人認証データの登録、およびこれらの項目の入力装置が接続されている場合であっても、それらの中から任意の項目、例えばパスワードのみを選択して照合を行うことができる。

【0018】請求項 3 に記載した発明においては、例えば、選択された入力装置が故障している場合や、何らかの原因で使用可能状態が外れた状態である場合に他の項目が代用されて用いられるため、システムの動作が停止してしまうことがない。

【0019】

【実施例】図 1 はこの発明の実施例に係る個人認証システムの構成例を示す図である。

【0020】ホストコンピュータ 1 には複数の CAT 端末 2 a, 2 b, … が接続されている。各 CAT 端末 2 a, 2 b, … には個人認証データを入力装置として、IC カードを挿入してその読み取りを行うための IC カード読取部 3、磁気カードのデータの読み取りを行う磁気カード読取部 4 が必要に応じて備えられるとともに、

パスワード入力用のキー（通常は、暗証番号を入力するためのテンキー）を有するキーパッド（ピンパッド）

5、サイン入力用のタブレット 6、指紋入力用の指紋読取装置 7 が必要に応じて接続されている。なお入力装置は個人を認証するためのデータが入力できるものであればよく、他に、声紋をチェックするための音声入力装置等が接続可能である。

【0021】IC カード読取部 3、磁気カード読取部 4 に挿入される IC カード、磁気カードにはそれぞれ個人を認証するための個人認証データや識別番号等の個人データが記憶されている。IC カードには識別番号、有効期限、パスワード等の通常のデータの他に、サイン（筆跡）、指紋等の高度な個人認証データも記憶されている。また磁気カードには通常のデータ、すなわち識別番号、有効期限や、パスワード等の簡単な個人認証データが記憶されている。したがって、IC カードを所有している個人に対しては識別番号、パスワードによるチェックの他に、サインや指紋の照合によるチェックも行うことができ、個人認識の確実性が向上する。

【0022】しかし、IC カードはそれだけで高価であるばかりでなく、サイン、指紋の照合を行うためにはそれらの入力装置、照合装置が必要であり、コスト高になる。一方、磁気カードを所有している個人に対しては識別番号、パスワードのチェックや目視によるサイン確認を行えるだけであるので個人認識の確実性はあまり高くないが、コスト的には安価な構成となる。

【0023】個人は必要に応じて IC カードまたは磁気カードのいずれかを所有することになるが、コストとの兼ね合いから、高度なセキュリティ性が要求される場合には IC カード、普通程度のセキュリティ性が必要な場合には磁気カードが用いられる。例えば、カードがクレジットカード等の金融取引カードである場合には、高額の取引を行う可能性がある顧客は IC カードを所持し、所定金額以下の取引のみの場合には磁気カードを所有することが考えられる。また企業内等での入退室チェックの場合には、重要度の高い部屋への入退室を行う者については IC カードを所有し、通常の部屋への入退室を行う者については磁気カードを所有することが考えられる。

【0024】なおこの実施例では個人認証データを IC カード、磁気カード内に記憶しているが、CAT 端末 2 に記憶したり、ホストコンピュータ 1 に記憶しておいてもよい。ホストコンピュータ 1 に記憶した場合には、照合時に CAT 端末 2 とホストコンピュータ 1 とが通信を行うことで照合を実行する。すなわち、上記の例では個人データ登録手段を IC カードや磁気カードが有しているが、該個人データ登録手段を CAT 端末 2 やホストコンピュータが備えていてもよい。

【0025】前記したように、CAT 端末 2 a, 2 b, … のそれぞれは必要に応じて IC カード読取部 3、磁

気カード読取部4、キーパッド5、タブレット6、指紋読取装置7等のデータ入力部を有している。図2はCAT端末の構成例を示す図、図3はCAT端末のブロック図である。

【0026】CAT端末2にはICカード読取部3、磁気カード読取部4、キーパッド5、タブレット6、指紋読取装置7等の入力装置がそれぞれスイッチSW1～SW5、コネクタ25a～25eを介して接続可能になっている。したがって必要な入力装置のみをコネクタ25a～25eを用いて接続することができる。例えば、金融取引システムの場合、接続する入力装置をそのCAT端末で取り扱う金額に応じて設定することができ、例えば、ごく小額の取り引きのみを行う端末の場合には簡易チェックを行うために、磁気カード読取部4のみを備えていても良いし、キーパッド5等も追加して備えてもよい。また、高額の取引を行う可能性のある端末の場合にはより高度なチェックを行うために、ICカード読取部3、および個人認証の確実性の高いサイン照合用のタブレット6や、指紋照合用の指紋読取装置7が追加してもよい。企業内等での入退室チェックを行うシステムの場合も同様で、簡易チェックで良い場合にはパスワード入力のためのキーパッド5のみ、磁気カード読取部4のみ、としたり、これらを組み合わせてみてもよいし、高度なセキュリティ性を要する場合にはICカード読取部3と、サインや指紋の照合を行うためのタブレット6や指紋読取装置7を備えてもよい。ただし、サイン入力用のタブレット6、指紋入力用の指紋読取装置7を接続する場合で、ICカード内にサインや指紋の個人データを記憶した場合にはICカード読取部4は必須となる。

【0027】また、コネクタにより接続した入力装置でもスイッチSW1～SW5をオン／オフすることによって接続状態を有効／無効にすることができる。このスイッチSW1～SW5は、例えば、入力装置のいずれかが故障した場合にその装置をオフしたり、例えばいずれかの入力装置を用いた方法で不正が発生してその装置による照合を停止する場合にオフしたりする場合に用いられる。コネクタ25a～25e、スイッチSW1～SW5が請求項1に記載した入力装置選択手段に対応する。

【0028】このように必要に応じてCAT端末ごとにデータ入力部を適宜設定できるため、例えば小額の取り引きしか行わない端末に、ICカード読取部3やタブレット6、指紋読取装置7等の高価な装置を備える必要がなく、システムが必要以上に高価になってしまうのを防止することができる。またパスワード、磁気カード、ICカードのいずれを用いても個人チェックが可能ないようにしているため、例えば小額の取り引きしか行わない顧客に対しては磁気カードを発行して、高価なICカードの使用を避けることができる。

【0029】CAT端末2は、CAT端末および該CAT端末に接続された各入力装置の処理動作を制御するC

PU21、処理プログラムを記憶するROM22、各入力装置の選択条件等を記憶するRAM23、前記各入力装置の選択条件を入力するための選択条件入力設定部24、ホストコンピュータ1との通信を行うためのモデム26や、ディスプレイ10、取引金額等の入力を行うためのキーパネル11を有している。選択条件入力設定部24、および、RAM23の選択条件の記憶部が請求項2に記載の照合項目選択手段に対応する。

【0030】選択条件入力設定部24は例えば端末の設置時や、必要に応じたメンテナンス時等に入力装置の選択条件を入力する部分である。例えば、金融取引装置では入力された金額ごとに個人認証方法が設定されて入力されたり、CAT端末を設置した場所に応じて個人認証方法が設定されて入力される。また例えば、入退室チェックの場合には重要度に応じて個人認証方法が設定される。なおこの入力時、同時に、選択条件入力設定部24からは、各入力装置の代用順も入力される。例えばICカード読取部が使用不可な状態のときには磁気カード読取部が代用される、というように代用する認証方法が入力される。そして設定された選択条件に応じて個人認証処理が実行される。

【0031】このシステムの動作手順を説明する。図4～図9はその処理手順を示すフローチャートであり、金融取引において取引金額高に応じて個人認証方法を選択するように選択条件入力設定部24から入力された場合の状態を示している。

【0032】まず、CAT端末2の電源がオンされると初期化処理を行い、それとともに接続されている各入力装置が使用可能であるかどうかを検証する(n51→n52)。そして異常がなければ入力待ち状態へと進むが、使用不可能な装置がある場合には、例えば『〇〇が使用不可能です』を表示する等の警告動作を行い、続行を示す入力がされるまで、所定時間待機する(n53→n54→n55→n56)。もし、所定時間内に続行を示す入力がされなかった場合にはそのままエラー処理となるが、続行が入力がされた場合には該当する部分の入力装置を代用させて設定する(n57)。例えば、いま、選択条件入力設定部24から入力された条件が、小額取引の場合にはパスワード照合のみを行うことであるとする。ところが入力装置としてパスワードの入力装置(キーパッド5)が使用不可能であるとする、予め選択条件入力設定部24から入力されているデータに基づいてパスワードの入力装置の他のものに代用させる。例えば、代用としてサインの照合が設定されている場合にはパスワードに代えてサインの照合を設定し、この条件を該CAT端末2の電源オフまでの間選択条件として記憶する。このようにし代用設定された装置について上記と同様に検証を行い、異常がなければ入力待ち状態になる(n58→n59→n60)。

【0033】次に取引処理時の手順を説明する。

【0034】まず取引の前処理として、取り引きの種類、金額等の入力を行う(n1)。種類は例えば、クレジットの場合であると『売上げ』等であり、銀行のカードであると『引出し』等である。そしてカード(磁気カードまたはICカード)が挿入されると、そのカードに記載されている識別番号、有効期限等を読み取って、該CAT端末での使用の可否のチェック、有効期限チェック、ネガチェック、預信限度額のチェック等を行う(n2→n3)。通常、CAT端末での使用の可否チェック、有効期限チェック等の簡単なチェックはCAT端末自身で行うが、他のネガチェック、預信限度額チェック等の複雑なチェックはホストコンピュータ1へ識別番号を送信して、ホストコンピュータ1側で行われる。チェック結果が正常な場合には、照合項目の設定処理へと進むが、チェック結果に異常があった場合、例えば有効期限切れや預信限度額をオーバーしていた場合等には取り引きの解除処理を行う(n4→n6, n5)。取引解除処理は、CAT端末のディスプレイ10にエラー表示を行うとともに、ICカード9を取り込んでいた場合にはそのICカードの非活性化処理および排出を行う。

【0035】照合項目の設定処理は図6に示すように、n1において入力された取引金額に応じて照合項目を選択設定する(n21→n22, n23, n24)。

【0036】n6で照合項目が設定されるとそれに応じてパスワード、サイン、指紋のそれぞれの照合をCAT端末内、ICカード内、またはホストコンピュータ内で行う(n8→n9, n10→n11, n12→n13)。

【0037】例えばパスワードの照合はCAT端末内で行う。パスワードの照合は図5に示すように、磁気カードまたはICカードから読み込んだパスワードと、キーパッド5から入力されたパスワードとを照合し、両者が一致すればメインフローへと戻る(n31→n32→n33→n34)。一方、両者が一致しない場合には数回のリトライを行うが、それでも一致しない場合にはエラー処理として取引解除処理を行う(n5)。このリトライ回数は、CAT端末において適宜設定される。なお、磁気カード8やICカード9にパスワードが記載されていない場合にもエラーを判定して取引解除となる(n5)。この実施例ではパスワードの照合をCAT端末内で行っているが、パスワードを予めホストコンピュータ1内に記憶しておいて、ホストコンピュータ1内で照合を行ってもよく、また、ICカードを用いる場合にはICカード内で照合を行ってもよい。

【0038】サインや指紋の照合はICカード内で行われる。例えばサインの照合は図6に示すように、CAT端末のタブレット6からサインが入力されると、ICカード内で照合が行われる(n41→n42→n43→n

44, n45→n46)。また指紋の照合も図7に示すように、CAT端末の指紋読取装置7から指紋が入力されると、ICカード内で指紋の照合が行われる。

【0039】以上のような照合処理により個人の認証が行われた場合には取引を許可して取引許可処理を実行する(n14)。すなわち、取り引きのためのデータ処理を行い、その結果をホストコンピュータに送信したり、ICカードに書き込んだ後、ICカードの排出処理等を行う。

【0040】以上のように必要に応じて適宜個人の照合項目が選択されて照合処理が行われる。これによって小額取引時等の高度な認証が不必要な場合等には簡易な認証のみを行うことができ、ランニングコストを安価にするとともにチェック時間も短縮でき、さらに、小額取引時等には指紋チェック等の顧客に対するイメージが悪い項目を削除することができ、顧客に対するサービス性の低下も防止できる。

【0041】

【発明の効果】請求項1, 2に示した発明によれば、必要に応じて照合項目を設定することが可能になるため、例えば簡易的な認証だけで良い場所や場面では簡易認証を行ってシステムコストまたはランニングコストを安価にすることができ、また例えば高度な認証を必要とする場所や場面では高度な認証を行ってセキュリティ性を向上させることができる。

【0042】また請求項3に示した発明によれば、一つの照合項目が使用不可能な場合には他の項目で代用して照合が行われるため、システム自体がストップしてしまうことがない。

【図面の簡単な説明】

【図1】この発明の実施例である金融機関での個人認証システムの構成例を示すブロック図である。

【図2】同システムのCAT端末の構成例を示す図である。

【図3】同CAT端末の要部ブロック図である。

【図4】同CAT端末の動作開始時の処理手順を示すフローチャートである。

【図5】同システムにおける金融取引手順例を示すフローチャートである。

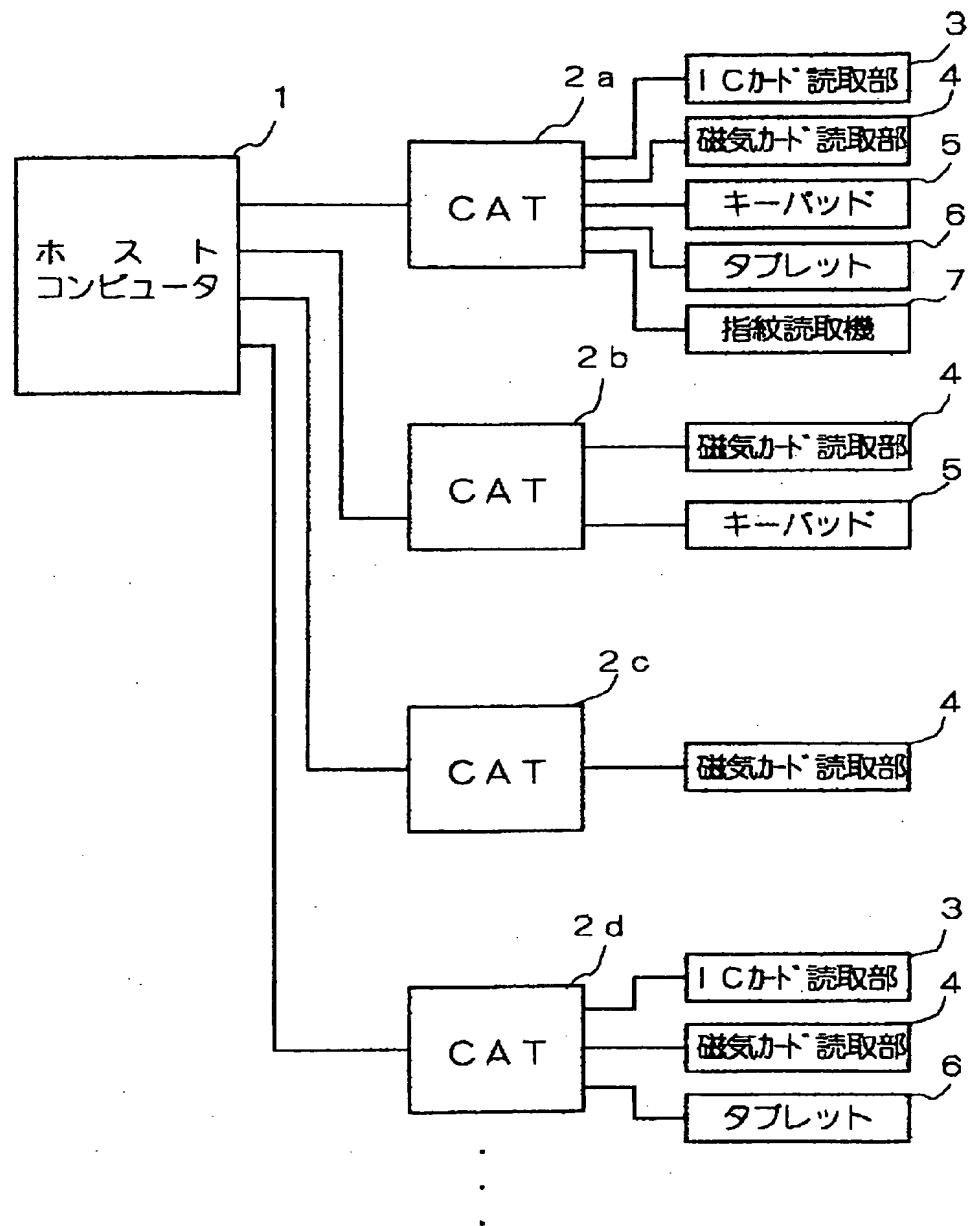
【図6】同システムにおける照合項目の設定手順例を示すフローチャートである。

【図7】同システムにおける個人認証の処理手順を示すフローチャートである。

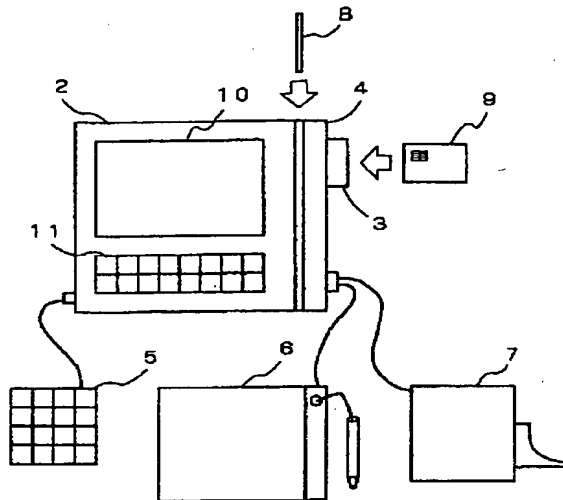
【図8】同システムにおける個人認証の処理手順を示すフローチャートである。

【図9】同システムにおける個人認証の処理手順を示すフローチャートである。

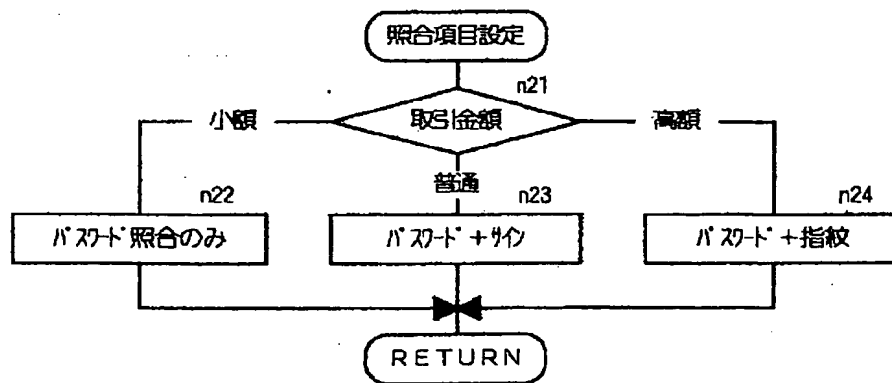
【図1】



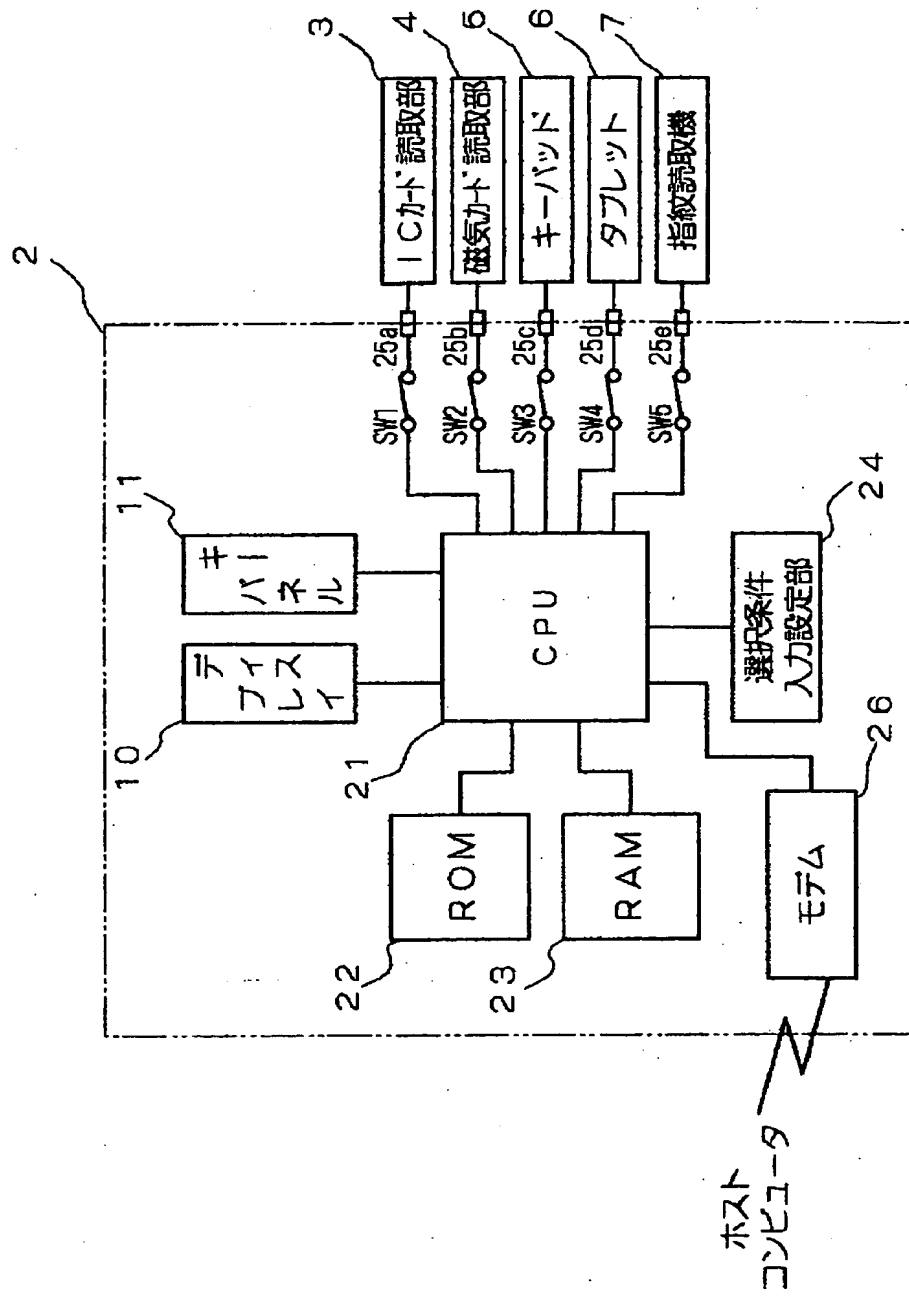
【図 2】



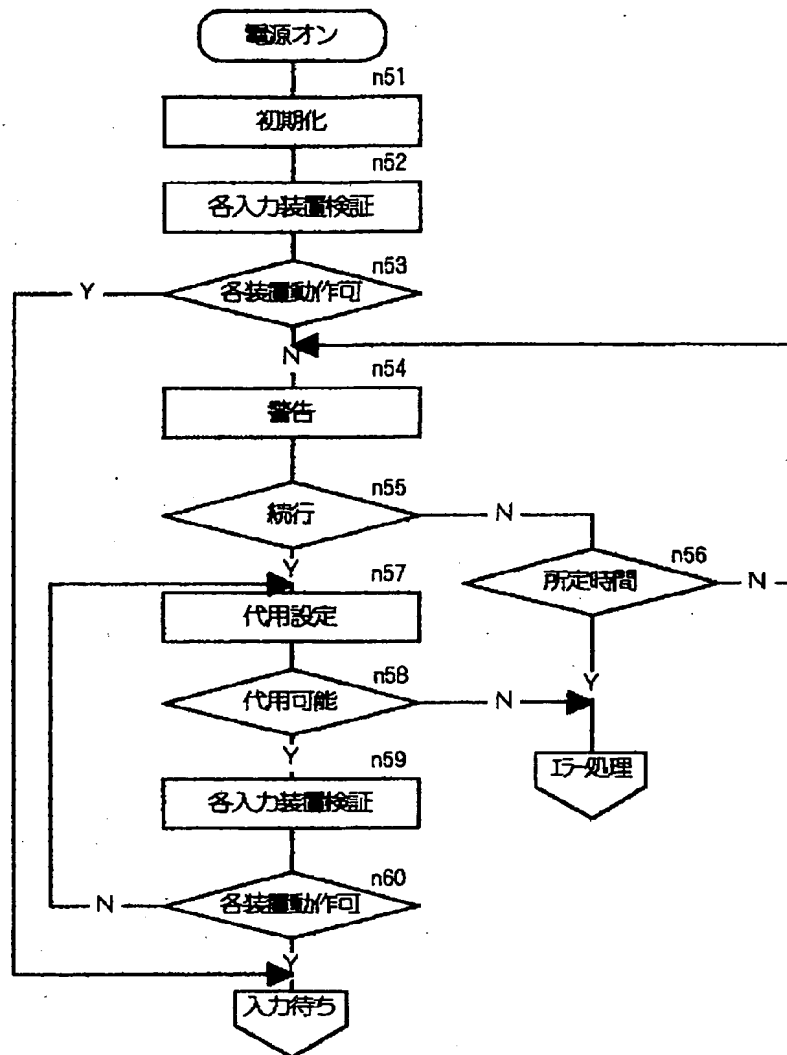
【図 6】



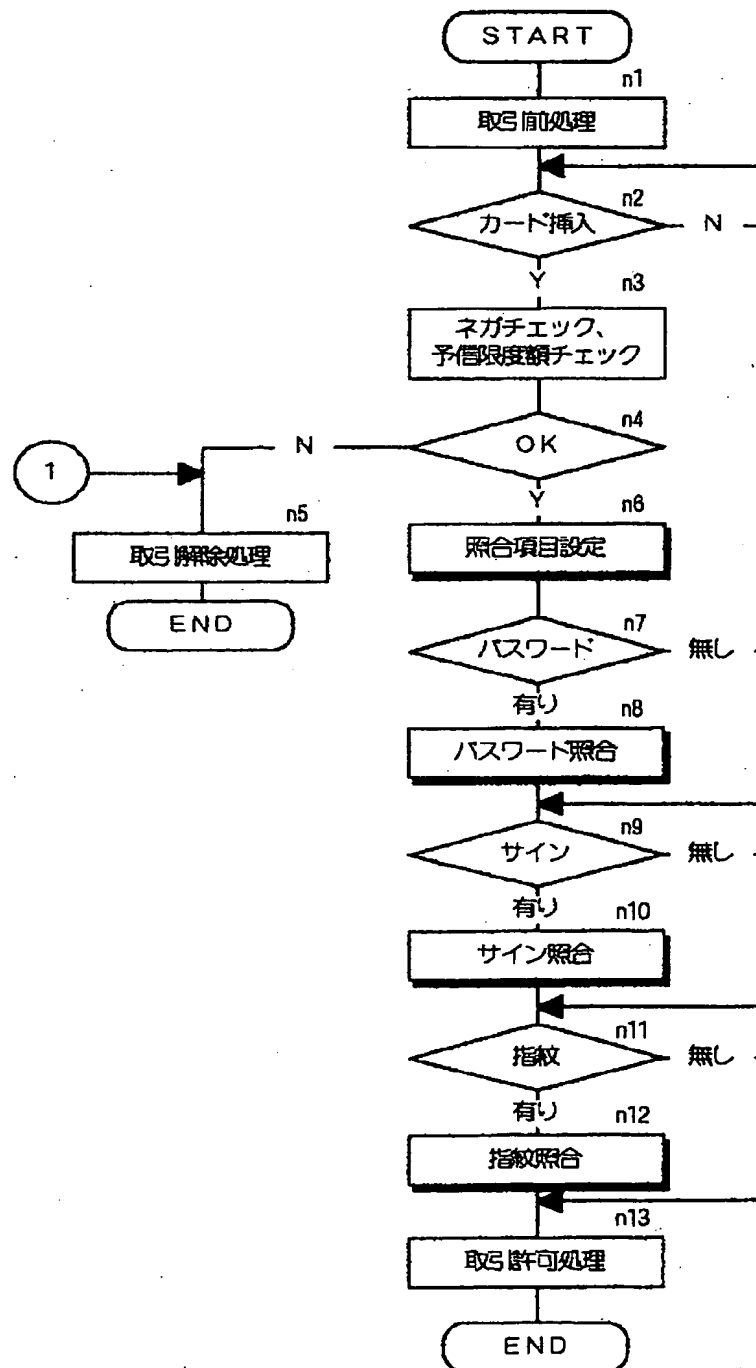
【図 3】



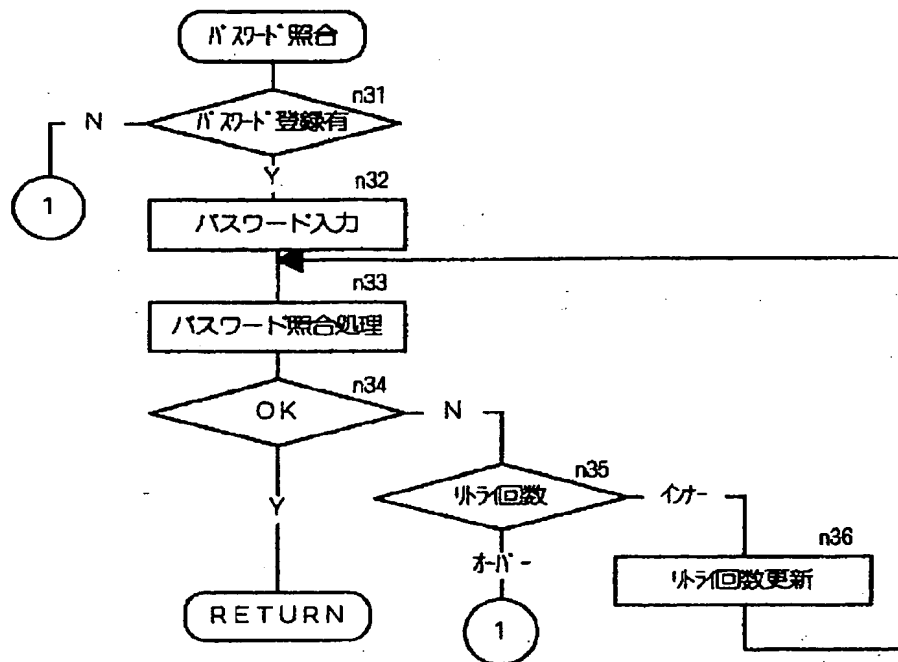
【図 4】



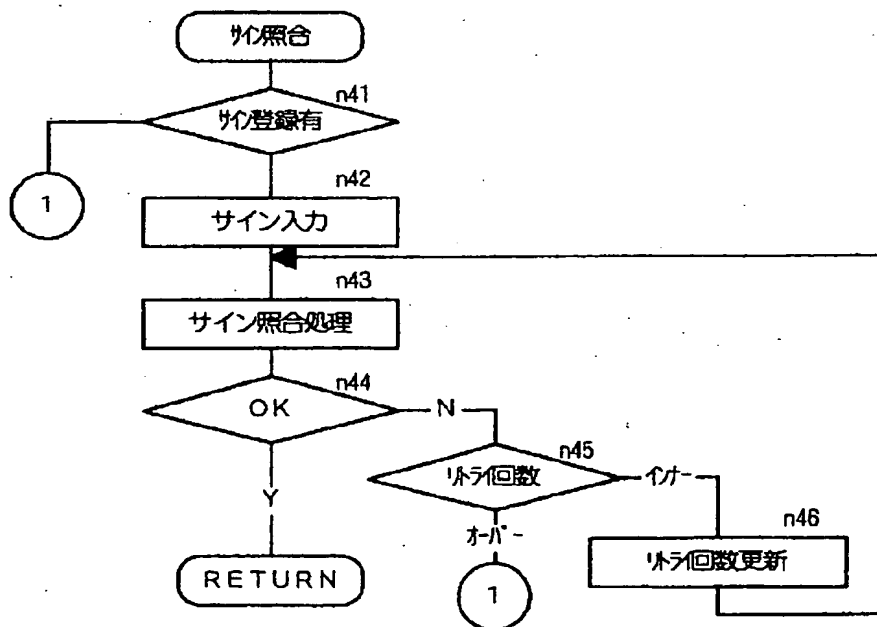
【図 5】



【図 7】



【図 8】



【図 9】

